BURSOR & FISHER, P.A.
Sarah N. Westcot (State Bar No. 264916)
701 Brickell Avenue, Suite 2100
Miami, FL 33133
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: swestcot@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

L.B., individually and on behalf of all other persons similarly situated,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

Case No. 5:24-cv-06832-EJD

PLAINTIFF'S OPPOSITION TO DEFENDANT LINKEDIN CORPORATION'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT

Date: January 9, 2025
Time: 9:00 a.m.
Dept: Courtroom 4, 5th Fl.
Judge: Hon. Edward J. Davila
Trial Date: TBD
Date Action Filed: August 20, 2024

TABLE OF CONTENTS

PAGE(S)

STATEMENT OF ISSUES TO BE DECIDED PER CIVIL L. R. 7-4(a)(3) 1

I. INTRODUCTION 1

II. STATEMENT OF FACTS 2

III. ARGUMENT 4

A. Plaintiff States a Claim Under CIPA § 631 4

1. LinkedIn Was Not a Party to the Communications Between Plaintiff and ReflexMD, It Was an Eavesdropper. 4

2. The First Clause of CIPA § 631(a) Applies to Defendant's Online Wiretaps. 8

3. Plaintiff Plausibly Alleges a Claim Under the Second Clause of CIPA § 631(a). 9

4. Plaintiff Plausibly Pleads a Claim Under the Third Clause of CIPA § 631(a) 12

B. Plaintiff States a Claim Under CIPA § 632 13

C. Plaintiff Adequately Alleges That Defendant Intercepted the "Content" of Her Communications with The Website 17

D. Plaintiff States a Claim for Invasion of Privacy Under the California Constitution 18

IV. CONCLUSION 23

TABLE OF AUTHORITIES

PAGE(S)

CASES

Brodsky v. Apple Inc.,
445 F. Supp. 3d 110 (N.D. Cal. 2020) 9, 17

Cousin v. Sharp Healthcare,
702 F. Supp. 3d 967 (S.D. Cal. 2023) 18, 19

Doe I v. Google LLC,
2024 WL 3490744 (N.D. Cal. July 22, 2024) 8

Doe v. Meta Platforms, Inc.,
690 F. Supp. 3d 1064 (N.D. Cal. 2023) ..... passim

Esparza v. Kohl's, Inc.,
723 F. Supp. 3d 934 (S.D. Cal. 2024) 4

Gladstone v. Amazon Web Servs., Inc.,
2024 WL 3276490 (W.D. Wash. July 2, 2024) 7, 11

Graham v. Noom, Inc.,
533 F. Supp. 3d 823 (N.D. Cal. 2021) 7

Heerde v. Learfield Commc'ns, LLC,
2024 WL 3573874 (C.D. Cal. July 19, 2024) 4, 7

Heiting v. Taro Pharms. USA, Inc.,
2024 WL 1626114 (C.D. Cal. Apr. 2, 2024) 11

Hernandez v. Hillsides, Inc.,
47 Cal. 4th 272 (2009) 18

In re Facebook, Inc. Internet Tracking Litig.,
956 F.3d 589 (9th Cir. 2020) 18, 20, 21, 22

In re Google Assistant Priv. Litig.,
457 F. Supp. 3d 797 (N.D. Cal. 2020) 15

In re Google Location Hist. Litig.,
514 F. Supp. 3d 1147 (N.D. Cal. 2021) 21

In re Meta Pixel Healthcare Litig.,
647 F. Supp. 3d 778 (N.D. Cal. 2022) ..... passim

In re Nickelodeon Consumer Priv. Litig.,
827 F.3d 262 (3d Cir. 2016) 23

In re Vizio, Inc., Consumer Priv. Litig.,
238 F. Supp. 3d 1204 (C.D. Cal. 2017) 23

Jackson v. LinkedIn Corp.,
2024 WL 3823806 (N.D. Cal. Aug. 13, 2024) ..... passim

Javier v. Assurance IQ, LLC,
649 F. Supp. 3d 891 (N.D. Cal. 2023) 4, 7

Javier v. Assurance IQ, LLC,
2022 WL 1744107 (9th Cir. May 31, 2022) 9

Kauffman v. Papa John's Int'l, Inc.,
2024 WL 171363 (S.D. Cal. Jan. 12, 2024) 4, 9

Libman v. Apple, Inc.,
2024 WL 4314791 (N.D. Cal. Sept. 26, 2024) 16

Mastel v. Miniclip SA,
549 F. Supp. 3d 1129 (E.D. Cal. 2021) 21

Matera v. Google Inc.,
2016 WL 8200619 (N.D. Cal. Aug. 12, 2016) 9

Navarro v. Block,
250 F.3d 729 (9th Cir. 2001) 13

Norman-Bloodsaw v. Lawrence Berkeley Lab'y,
135 F.3d 1260 (9th Cir. 1998) 17, 18

Oddo v. United Techs. Corp.,
2022 WL 577663 (C.D. Cal. Jan. 3, 2022) 22

Opperman v. Path,
87 F. Supp. 3d 1018 (N.D. Cal. 2014) 22

People v. Superior Ct. of Los Angeles Cnty.,
70 Cal. 2d 123 (1969) 15

Revitch v. New Moosejaw, LLC,
2019 WL 5485330 (N.D. Cal. Oct. 23, 2019) 17

Robbins v. Mscripts, LLC,
2023 WL 5723220 (N.D. Cal. Sept. 5, 2023) 20, 22

Rojas v. HSBC Card Servs. Inc.,
20 Cal. App. 5th 427 (2018) 14, 15

Shah v. Fandom, Inc.,
2024 WL 4539577 (N.D. Cal. Oct. 21, 2024) 9

Smith v. Google, LLC,
2024 WL 2808270 (N.D. Cal. June 3, 2024) 4, 6, 7, 11

St. Aubin v. Carbon Health Techs., Inc.,
2024 WL 4369675 (N.D. Cal. Oct. 1, 2024) 8, 18

Valenzuela v. Nationwide Mut. Ins. Co.,
686 F. Supp. 3d 969 (C.D. Cal. 2023) 9, 11

Yockey v. Salesforce, Inc.,
2024 WL 3875785 (N.D. Cal. Aug. 16, 2024) 16

Yoon v. Lululemon USA, Inc.,
549 F. Supp. 3d 1073 (C.D. Cal. 2021) 4

STATUTES

18 U.S.C. § 2510(8) 9, 17

42 U.S.C. § 1320d ..... passim

Cal. Penal Code § 632 ..... 13, 14, 15, 16

REGULATIONS

45 C.F.R. § 160 ..... 14, 18, 19

45 C.F.R. § 164 ..... 14, 17, 18, 22

STATEMENT OF ISSUES TO BE DECIDED PER CIVIL L. R. 7-4(a)(3)

1. Whether Plaintiff L.B. ("Plaintiff") states a claim under the California Invasion of Privacy Act ("CIPA") § 631(a) and § 632 where Defendant LinkedIn Corporation ("Defendant" or "LinkedIn") eavesdropped on Plaintiff's and class members' communications with ReflexMD, Inc. ("ReflexMD") involving sensitive and private health information, via ReflexMD's website, www.reflexmd.com (the "Website"), using the LinkedIn Insight Tag, without consent.

2. Whether Plaintiff states a claim for invasion of privacy under the California Constitution where Plaintiff had a reasonable expectation of privacy that the protected health information she shared with the Website would remain confidential between her and ReflexMD, and where Defendant intercepted Plaintiff's said information.

I. INTRODUCTION

Plaintiff hereby opposes Defendant's Motion to Dismiss Plaintiff's Complaint (ECF No. 13) ("MTD"). Plaintiff states a claim under CIPA § 631(a) and § 632 and for invasion of privacy under California's Constitution because Defendant intentionally, and without the consent of Plaintiff and class members, intercepted sensitive and confidential communications between Plaintiff (and class members) and third party ReflexMD, via ReflexMD's Website. Specifically, Defendant intercepted Plaintiff's and class members' confidential prescription information because Defendant's software, the LinkedIn Insight Tag, is embedded on the Website, which captured Plaintiff's and class members' interactions with the Website, including their purchase of prescription medication, Semaglutide. Defendant then uses the information it collects by incorporating it into its advertising machinery which functions to place Plaintiff and class members into targeted audiences for advertisers of similar products by serving them targeted advertising on the LinkedIn platform. Defendant makes the LinkedIn Insight Tag free for website owners to use for exactly that reason, namely, so that it can surreptitiously receive information from website interactions, connect those interactions to a specific LinkedIn user, and then generate highly specific audience segments which Defendant then uses to sell advertising.

As a result of Defendant's unlawful conduct, Plaintiff brings the present action on behalf of herself and a class of "all LinkedIn account holders in the United States who purchased Semaglutide

on www.reflexmd.com." *See* Complaint ¶ 48 (ECF No. 1). Plaintiff brings claims against Defendant for (1) violation of CIPA § 631(a), (2) violation of CIPA § 632, and (3) invasion of privacy under the California Constitution. *Id.* ¶¶ 58-88.

Notably, the Honorable P. Casey Pitts recently considered a similar case involving a CIPA § 631 claim related to Defendant's use of the LinkedIn Insight Tag on a different website. Judge Pitts denied Defendant's motion to dismiss while rejecting many of the same arguments Defendant makes here. *See, e.g.*, *Jackson v. LinkedIn Corp.*, 2024 WL 3823806 (N.D. Cal. Aug. 13, 2024). The same outcome is appropriate here.

II. STATEMENT OF FACTS

ReflexMD offers one product on its Website, a prescription weight loss medication called Semaglutide, which is a Glucagon-like peptide ("GLP-1"). Complaint ("Compl.") ¶ 35 (ECF No. 1, Ex. 1 to Notice of Removal). Because Semaglitude is a prescription medication, consumers must complete a medical exam or survey from a healthcare provider to qualify for the medication. *Id.* ¶¶ 4, 36. The survey on the Website includes private questions about consumers' health and weight loss goals. *Id.* ¶¶ 37, 39-41. Despite collecting private health information from its customers, ReflexMD embedded Defendant's LinkedIn Insight Tag on its Website, which enabled LinkedIn to intercept Website visitor's confidential health and prescription information to monetize the data for targeted advertising on LinkedIn. *Id.* ¶ 38.

Defendant's LinkedIn Insight Tag is a code snippet added to an advertiser's website (here reflexmd.com) which provides tools for the advertiser to optimize advertising campaigns, retarget Website visitors who did not make a purchase, and "learn about [its] audiences." *Id.* ¶ 21. The current iteration of Defendant's LinkedIn Insight Tag is a JavaScript-based code which allows the LinkedIn Insight Tag to (1) track users and (2) circumvent third-party cookie blockers because it is a first-party cookie embedded within the Website itself. *Id.* ¶ 22. This means that even if third party cookies are blocked, the LinkedIn Insight Tag still captures consumers' information, frustrating the privacy choices of consumers. When a user who has signed in to LinkedIn (even if the user subsequently logs out) is browsing the Website (where the LinkedIn Insight Tag has been embedded), an HTTP request is sent using cookies, which includes information about the user's

actions on the Website and data that differentiates users from one another which can be used to link that data to the user's LinkedIn profile. *Id.* ¶¶ 23-24. The cookies are used by LinkedIn to identify its members for Defendant's own advertising purposes. *Id.* ¶¶ 25-27. Through the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more. *Id.* ¶ 16. The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network. *Id.* ¶ 17.

Through use of the LinkedIn Insight Tag, Defendant tracked Plaintiff's and class members' activity from the moment they navigated to the Website, including "click" events (information about which page on the ReflexMD Website the patients viewed and the selections they made on the particular web page). *Id.* ¶ 43. In short, LinkedIn intercepts nearly all consumers' confidential communications with ReflexMD when they are completing their medical survey on the Website, including communications revealing Plaintiff's and class members' gender, weight loss goals, and purchase history (which is significant because there is only one Product, Semaglutide, available for purchase on the Website). *Id.* ¶¶ 35, 44.

Plaintiff is a LinkedIn user. Compl. ¶ 5. Plaintiff purchased Semaglutide from ReflexMD via the Website in approximately June 2024. *Id.* ¶ 6. Unbeknownst to Plaintiff, Defendant intentionally intercepted her communications with the Website via the LinkedIn Insight Tag. *Id.* Defendant used the LinkedIn Insight Tag to track Plaintiff and intercept her communications with ReflexMD, including communications that contained confidential prescription information. *Id.* ReflexMD patients, including Plaintiff, were unaware that the LinkedIn Insight Tag was installed on the Website. Plaintiff and class members never consented, agreed, authorized, or otherwise permitted LinkedIn to intercept their confidential health and prescription information and/or sell her data to advertisers. *Id.* ¶¶ 6, 46.

III. ARGUMENT

A. Plaintiff States a Claim Under CIPA § 631

CIPA § 631 creates avenues for relief where a person: (1) "by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection ... with any telegraph or telephone wire, line, cable, or instrument"; (2) "willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit"; and (3) "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained[.]" *Heerde v. Learfield Commc'ns, LLC*, 2024 WL 3573874, at *4 (C.D. Cal. July 19, 2024) (quoting *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 897 (N.D. Cal. 2023)). Here, Plaintiff plausibly states a claim under each of the above-mentioned prongs of CIPA. CIPA § 637.2 provides a civil cause of action to anyone who violates § 631. *Smith v. Google, LLC*, 2024 WL 2808270, at *3 (N.D. Cal. June 3, 2024).

1. LinkedIn Was Not a Party to the Communications Between Plaintiff and ReflexMD, It Was an Eavesdropper.

Defendant argues that Plaintiff "fails to allege that LinkedIn acted as anything more than an extension of and service provider to ReflexMD, which was a party to the alleged communications." MTD at 6. That is wrong.

As a threshold matter, the question of whether Defendant is a party to the communication or a third-party eavesdropper is a question of fact not suitable for determination on a motion to dismiss. *Kauffman v. Papa John's Int'l, Inc.*, 2024 WL 171363, at *7 (S.D. Cal. Jan. 12, 2024) ("Whether FullStory acts akin to a tape recorder or whether its actions are closer to 'an eavesdropper standing outside the door' is a question of fact which is better answered after discovery into the session replay technical context of the case."); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) ("The question thus becomes, in analogue terms: is Quantum Metric a tape recorder held by Lululemon, or is it an eavesdropper standing outside the door? This is a question of fact for a jury, best answered after discovery into the storage mechanics of Session Replay."); *Esparza v. Kohl's, Inc.*, 723 F. Supp. 3d 934, 942 (S.D. Cal. 2024) ("The Court finds here that whether ASI acts akin to

a tape recorder or whether its actions are closer to 'an eavesdropper standing outside the door' is a question of fact which is better answered after discovery.").

Regardless, Plaintiff alleges that she "never consented, agreed, authorized, or otherwise permitted LinkedIn to intercept her confidential health and prescription information." Compl. ¶ 46; *see also id.* ¶ 75 ("Plaintiff and Class Members expected their communications to ReflexMD to be confined to ReflexMD in part, due to the protected nature of the health information at issue. Plaintiff and Class Members did not expect third parties, like LinkedIn, to secretly eavesdrop upon or record this confidential information and their communications."). Despite this, Defendant has intercepted Plaintiff's and class members' communications with ReflexMD and used the data itself "to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network." Compl. ¶ 17.

In short, Defendant uses the data it receives from the LinkedIn Insight Tag to group users into audience groups, which it then sells to advertisers by displaying their ads to the targeted groups it created through the intercepted data from the Website (and other websites using the LinkedIn Insight Tag). *See* Compl. ¶ 38 ("Through the LinkedIn Insight Tag, Defendant intercepted consumers confidential prescription information in order to monetize that data for targeted advertising."). Defendant's use of the intercepted data for its own advertising purposes brings it outside the scope of a mere "vendor." That the LinkedIn Insight Tag may have been installed by ReflexMD (MTD at 7) is irrelevant to the analysis because the question is whether LinkedIn made use of the data for its own purposes, regardless of who installed the tag. And Plaintiff specifically alleges that LinkedIn used the information gleaned from the LinkedIn Insight Tag for its own marketing purposes (Compl. ¶¶ 17, 24-27, 38), which establishes that Defendant was a third-party eavesdropper under CIPA. Defendant was not a mere service provider. *See id.* ¶ 67 ("LinkedIn used or attempted to use the communications and information [it] received through their tracking technology, including to supply advertising services.").

Judge Pitts, considering a similar case involving a CIPA § 631 claim related to use of the LinkedIn Insight Tag on a different website, squarely rejected Defendant's same argument, reasoning that "LinkedIn received this sensitive data and read and used it for its own marketing services."

Jackson v. LinkedIn Corp., 2024 WL 3823806, at *5 (N.D. Cal. Aug. 13, 2024). Plaintiff here makes nearly identical allegations as in *Jackson*, which led Judge Pitts to conclude that LinkedIn was more than just a vendor with respect to the LinkedIn Insight Tag. *Compare Jackson*, 2024 WL 3823806, at *5 ("LinkedIn's Marketing Services monetizes the collected data through the sale of [ads]."); *id.* ("LinkedIn is also learning the contents of communications between website users and the DMV. This enables advertisers to target users with relevant content or advertisement[s] using the personal information and data that LinkedIn harvested.") *with* Compl. ¶ 17 ("The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network."); *id.* ¶ 38 ("Through the LinkedIn Insight Tag, Defendant intercepted consumers confidential prescription information in order to monetize that data for targeted advertising.").[1] Defendant's "acquisition and review of the disability information by LinkedIn for advertising purposes qualifies as interception under CIPA." *Jackson*, 2024 WL 3823806, at *5.

In *Smith v. Google, LLC*, 2024 WL 2808270 (N.D. Cal. July 2, 2024), Judge Pitts reached the same conclusion regarding similar tracking software offered by Google. There, Google, like Defendant here, offered "tools that track how users interact with websites[,]" including "information about the user's browser, language, clicks, downloads, and form interactions, as well as the titles of webpages, and matches the information it collects with a user's location, gender, and general interests." *Id.* at *1. Also like the LinkedIn Insight Tag, the data collected by Google's tools was "sent in real time to Google, which store[d] the data and processe[d] it into reports." *Id.* Like LinkedIn here, Google benefitted from the collection of the data because Google used the "data to power its algorithms and learn about user habits." *Id.* And, as Defendant does here, Google argued that it was merely acting as a vendor and providing software tools for the benefit of its customers, and therefore was not liable under CIPA § 631. *Id.* at *4 ("Google . . . argues that the Section 631

[1] Defendant's argument largely devolves into fact-based arguments and baseless contentions that Plaintiff's factual allegations regarding Defendant's use of the data are somehow "conclusory" (MTD at 7-8). But Defendant cannot escape the fact that nearly identical allegations regarding the *very same software* were upheld in *Jackson*. Defendant recognizes this and offers only the feeble assertion that "the Court erred" (MTD at 9), when in fact it did not.

claim should be dismissed because Google acted as a 'mere vendor' of a tool that allows websites to record their own interactions with their users.").

However, the *Smith* court rejected Google's argument, finding that Google reads and uses the collected data by: (1) using the data to power its algorithms; (2) gaining detailed information about its users; and (3) collecting and aggregating the data to present to its customers on a dashboard. *Id.* at *4. The court also noted that Google provides the tools for free, "suggesting that Google derives some benefit when websites use the tool." *Id.* The court concluded that "Google is not simply a vendor of a tool that websites can use to 'record' their own users' interactions on their websites, but rather that Google read or used the data collected about these users." *Id.* at *5. So too here, Defendant's LinkedIn Insight Tag records "click" events (Compl. ¶ 43), personal information regarding user's gender, weight loss goals, and purchase of Semaglutide (*id.* ¶ 44), and Defendant used the data for its own advertising purposes and to provide "in-depth campaign reporting" to advertisers using the LinkedIn Insight Tag (*id.* ¶ 21). As such, the *Smith* decision is directly analogous to this matter.

In both *Jackson* and *Smith*, Judge Pitts distinguished and declined to follow the primary authority cited by Defendant, *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021) (*see* MTD at 6), on the grounds that in both *Jackson* and *Smith*, Defendant and Google actually used the data for their own purposes, whereas in *Graham*, there were "no allegations here that FullStory intercepted and used the data itself." *Id.* at 832. This case is akin to *Jackson* (which also involved the same LinkedIn Insight Tag) and *Smith*, as Plaintiff alleges that Defendant used the data collected from the LinkedIn Insight Tag for its own marketing purposes. Compl. ¶¶ 17, 38; *see also Javier*, 649 F. Supp. 3d at 901 ("Javier has plausibly alleged that ActiveProspect is a third party under Section 631, and Defendants' argument that ActiveProspect is an 'extension' of Assurance does not provide a basis for dismissal at this stage."); *Gladstone v. Amazon Web Servs., Inc.*, 2024 WL 3276490, at *6 (W.D. Wash. July 2, 2024) ("Plaintiff's allegations demonstrate that Defendant has capabilities beyond that of a mere tape recorder, and there is no evidence that Defendant is incapable of using the data for any other purpose."); *Heerde*, 2024 WL 3573874, at *7 (agreeing with *Javier* and finding that "Plaintiffs allege plausibly Defendants were third-party eavesdroppers to Plaintiffs'

communications."); *Turner v. Nuance Commc'ns, Inc.*, 2024 WL 2750017, at *8-11 (N.D. Cal. May 28, 2024).

Defendant also relies on *Doe I v. Google LLC,* 2024 WL 3490744 (N.D. Cal. July 22, 2024), but that case is distinguishable. There, the court conceded that the "allegation that Google creates reports of user activity on a given web property does seem to support an inference that Google is doing more than simply acting as a tape recorder" but that the plaintiffs did not "adequately allege where on a web property the source code actually exists." *Id.* at *6. Here, by contrast, Plaintiff alleges in detail where on the ReflexMD Website the LinkedIn Insight Tag is embedded and the exact information transmitted to LinkedIn. Compl. ¶¶ 43-45. Of note, another court in the Northern District reached an alternative conclusion to that reached by the court in *Google* on similar facts, further undermining its viability. *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1078-80 (N.D. Cal. 2023), *motion to certify appeal denied*, 2024 WL 4375776 (N.D. Cal. Oct. 2, 2024).

Defendant argues that "even if Plaintiff's sparse allegations regarding LinkedIn's advertising services were sufficient to plead capability of use under *Javier*, her claims would still fail for an independent reason: None of those allegations are tethered to Plaintiff's alleged communications with ReflexMD." MTD at 9. This argument is baseless as Plaintiff alleges: (1) she purchased Semaglutide from the Website in approximately June 2024 (Compl. ¶ 6); (2) that unbeknownst to her, Defendant tracked her private activity on the Website using the LinkedIn Insight Tag (*id.*); (3) precisely how Defendant intercepts information from the Website (*id*. ¶¶ 43-45); and (4) that Defendant specifically intercepted communications between Plaintiff and the Website that contained "confidential prescription information" (*id.* ¶ 6).

2. The First Clause of CIPA § 631(a) Applies to Defendant's Online Wiretaps.

Defendant contends that Plaintiff cannot bring a claim under the first clause of CIPA § 631(a) because that section "prohibits telephonic wiretapping, which does not apply to the internet." MTD at 10 (quoting *St. Aubin v. Carbon Health Techs., Inc.*, 2024 WL 4369675, at *4 (N.D. Cal. Oct. 1, 2024)). Defendant is wrong. Indeed, in *Jackson*, Judge Pitts held that CIPA applied to the LinkedIn Insight Tag and explained that "Section 631 applies to 'new technologies' such as computers, email,

and the Internet." *Jackson*, 2024 WL 3823806, at *5 (quoting *Matera v. Google Inc.*, 2016 WL 8200619, at *20 (N.D. Cal. Aug. 12, 2016)). In *Matera*, the court correctly reasoned that the "California Supreme Court . . . regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." 2016 WL 8200619, at *20. After surveying California case law consistently applying this principle of law, the court in *Matera* concluded that "[b]ecause the California Supreme Court regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme, the Court is unpersuaded by Google's argument that CIPA can not apply to email because email did not exist at the time of CIPA's enactment." *Id.* In *Kauffman*, 2024 WL 171363, at *8, the court applied *Matera* and reasoned that "[r]eading the first clause of Section 631 to apply only to communications through a wire ignores the fact that a statute may be read to apply to new technologies . . ." *See also id.* ("[t]hough written in terms of wiretapping, § 631(a) applies to internet communications") (quoting *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022)); *Shah v. Fandom, Inc.*, 2024 WL 4539577, at *4 (N.D. Cal. Oct. 21, 2024) ("Giving effect to CIPA's broad statutory language is consistent with the California Legislature's stated intent to protect privacy interests, as well as the California courts' approach when applying statutes to new technologies.").

Plaintiff alleges that "LinkedIn, though the LinkedIn Insight Tag, intentionally tapped or made unauthorized connections with, the lines of internet communications between Plaintiff and Class Members and the ReflexMD Website without the consent of all parties to the communication." Compl. ¶ 65. Plaintiff therefore adequately pleads a violation of the first clause of CIPA.

3. Plaintiff Plausibly Alleges a Claim Under the Second Clause of CIPA § 631(a).

To plausibly allege a violation of the eavesdropping prong (second clause) of CIPA, a plaintiff must allege that the violator (1) read, or attempted to read, contents[2] of a message or similar communication; (2) without consent of all the parties; (3) while the message was in transit, passing over a wire, or being sent or received from within California; and (4) did so willingly. *See Valenzuela*

[2] "Contents" "include[ ] any information concerning the substance, purport, or meaning of [a] communication.'" *See* 18 U.S.C. § 2510(8); *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) ("The analysis for a violation of CIPA is the same as that under the federal Wiretap Act.") (citation omitted).

v. Nationwide Mut. Ins. Co., 686 F. Supp. 3d 969, 976–77 (C.D. Cal. 2023). Here, Plaintiff's allegations satisfy each element of her claim.

First, Plaintiff plausibly alleges that Defendant learned or attempted to learn the contents of her communications because, through the LinkedIn Insight Tag, Defendant intercepted the substantive communications between Plaintiff and the Website, which included Plaintiff's confidential health and prescription information. Compl. ¶ 6. Plaintiff, a purchaser of Semaglutide, interacted with Defendant's Website by completing the required survey and by purchasing the medication, and Defendant intercepted those communications and used them for the purpose of augmenting its own advertising services. *Id.* ¶¶ 6, 35-45; *see also id.* ¶¶ 17, 24-27, 38.

Defendant argues that "[a]t most, Plaintiff alleges that LinkedIn ***received*** her alleged communications, not that it read or attempted to learn their contents." MTD at 11. But Defendant's argument is belied by the factual allegations in the Complaint—namely, that Defendant read and used the contents of Plaintiff's communications for purposes of creating advertising audiences based on Plaintiff's communications with the Website and for purposes of organizing the data into metrics to be used by ReflexMD. Compl. ¶ 16 ("As a result of its activities and operation of the LinkedIn Insight Tag, LinkedIn is able to make extremely personal inferences about individuals' demographics, intent, behavior, engagement, interests, buying decisions, and more."); *id.* ¶ 17 ("The personal information and communications obtained by LinkedIn are used to fuel various services offered via LinkedIn's Marketing Solutions including Ad Targeting, Matched Audiences, Audience Expansion, and LinkedIn Audience Network."); *id.* ¶¶ 18-19; *id.* ¶ 21 (LinkedIn Insight Tag enables "in-depth campaign reporting").[3]

Second, Plaintiff did not consent to Defendant eavesdropping on her interactions with the Website. *Id.* ¶¶ 3, 6, 28, 62. Defendant does not contest this point.

Third, Plaintiff alleges that Defendant attempted to read or learn the contents of Plaintiff's communications with the Website while the same were in transit. *Id.* ¶ 66. To satisfy the so-called

[3] Defendant argues that "an analytics provider that offers a tool to allow customers to process their own data cannot be said to 'read' or 'learn' the contents of a communication." MTD at 11. But this is just a repackaged version of Defendant's vendor argument, which is wrong for the reasons set forth in Section III.A.1., above.

"in transit" requirement, Plaintiff need only "demonstrate a party intercepted the communication during its transmission, rather than once it was placed in electronic storage." *Heiting v. Taro Pharms. USA, Inc.*, 2024 WL 1626114, at *8 (C.D. Cal. Apr. 2, 2024). Here, Plaintiff more than plausibly explains how Defendant uses the LinkedIn Insight Tag to intercept Plaintiff's and class members' communications with the Website in real time, while they were in transit. *Id.* ¶¶ 23-25, 43-45. Specifically, Defendant intercepted Plaintiff's and class members' communications at the time that Plaintiff and class members input said communications into the Website, as the function of the LinkedIn Insight Tag duplicated the communications with the Website and sent the same to LinkedIn. *Id.* ¶¶ 23-25, 43-45. Plaintiff's allegations thereby place Defendant on sufficient notice of the basis of what is alleged. *See Valenzuela*, 686 F. Supp. 3d at 979 ("[T]he SAC makes quite clear that Valenzuela's allegation is that Akamai's code intercepts chat messages in real time and stores transcripts, which gives Nationwide plenty of notice on what is alleged . . . Nothing more than this combination of plausibility and notice is required at this stage."). Notably, in *Jackson*, the court concluded that the same LinkedIn Insight Tag at issue here violated the second clause of CIPA, concluding that the tag intercepts communications "in transit." 2024 WL 3823806, at *5-6.

Fourth, Plaintiff alleges that Defendant intercepted Plaintiff's communications willfully and intentionally. Compl. ¶¶ 3, 7, 33; *see also Jackson*, 2024 WL 3823806, at *5-6 (denying motion to dismiss based on the second clause of CIPA). Indeed, the very purpose and function of the LinkedIn Insight Tag is to intercept an individual's interaction with a website. *Id.* In other words, Defendant intends to intercept all information obtained through the LinkedIn Insight Tag. *See Meta Platforms*, 690 F. Supp. 3d at 1079 ("Meta's point that Pixel captures some data that healthcare entities may permissibly share with Meta might provide a defense to some portion of plaintiffs' CIPA claim, but it does not negate the plausible allegations that sensitive healthcare information is intentionally captured and transmitted to Meta."). Further, "[w]hether a person possesses the requisite intent under CIPA is generally a question of fact." *Gladstone*, 2024 WL 3276490, at *10; *see also Smith*, 2024 WL 2808270, at *5 ("While Google argues that judicially noticeable policy documents suggest that Google did not actually want to receive personally identifiable information and expressly prohibited

developers from transmitting such data, this presents a question of fact that the Court cannot resolve at this stage.").

Finally, Defendant argues that Plaintiff must allege the communication was sent or received within California. MTD at 12. Not so. Here, there is a choice of law provision between LinkedIn and its users favoring California law, and, even under a choice of law analysis, California law applies. Compl. ¶ 56. While Defendant argues that Plaintiff must allege that it intercepted her "communications to or from the state of California" (MTD at 12), it misreads the statute. The second clause of CIPA states: ". . . who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit **or** passing over any wire, line, or cable, **or** is being sent from, or received at any place within this state." CIPA § 631 (emphasis added). The statute is disjunctive, meaning that Plaintiff need only show that the communication was intercepted while in transit, which she has done. Further, courts considering choice of law arguments at the pleading stage have correctly declined to dismiss CIPA claims based on extraterritoriality arguments. *Meta Platforms*, 690 F. Supp. 3d at 1078–79.

4. Plaintiff Plausibly Pleads a Claim Under the Third Clause of CIPA § 631(a).

The third clause of CIPA creates liability where Defendant uses or attempts to use data unlawfully obtained in violation of either the first or second clauses of CIPA. Here, Defendant violated the third clause of CIPA because it used the data it unlawfully intercepted in violation of the first and second clauses of CIPA to learn sensitive, confidential information regarding its users (by intercepting information input by users onto the Website and connecting it to their LinkedIn account). *Meta Platforms*, 690 F. Supp. 3d at 1079-80; *Jackson*, 2024 WL 3823806 at *5-6. Defendant then uses the data to make highly specific audience segments for advertisers to target by serving them related advertising on the LinkedIn platform. Compl. ¶¶ 16-17, 23-27.

Defendant argues that Plaintiff's allegations regarding its use of the data are "conclusory." MTD at 13-14. That is wrong. Plaintiff alleges precisely how the LinkedIn Insight Tag works to intercept Plaintiff's and class members' information input on to the Website, and pleads facts, not

legal conclusions, regarding Defendant's use of the data, namely, to target LinkedIn account holders for advertising by using the intercepted data. Compl. ¶¶ 16-17, 23-27. These are allegations of fact that must be accepted as true at the pleading stage. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001) (explaining that "all material allegations of the complaint are accepted as true, as well as all reasonable inferences to be drawn from them").

B. Plaintiff States a Claim Under CIPA § 632

Cal. Penal Code § 632(a) states, in pertinent part:

> (a) A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500) per violation . . .

Cal. Penal Code § 632(c) defines "confidential communication" as:

> any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive, or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

Plaintiff states a claim under Cal. Penal Code § 632(a) because Defendant, without Plaintiff's consent, eavesdropped on Plaintiff's confidential communications with the Website, which included (1) sensitive personal and health information disclosed via the survey on the Website, and (2) Plaintiff's purchase of the Semaglutide medication on the Website, including prescription information. Compl. ¶¶ 6, 35-47, 74-75. The LinkedIn Insight Tag is an electronic recording device because it functions to electronically intercept and record Plaintiff's interactions with the Website. *Id.* ¶¶ 21-27, 38, 43-45. Plaintiff had a reasonable expectation of privacy when communicating with the Website because private health information is among the most sensitive information relevant to any individual, which is why disclosure of such information is heavily regulated by federal law. *See,*

e.g., 42 U.S.C. § 1320d-6; 45 C.F.R. Part 160 and 164. Plaintiff had every reason to believe that, when ordering prescription medication from ReflexMD (which is the only product offered on the Website), information conveyed by Plaintiff to ReflexMD would remain private as between those two parties, without an unknown third-party eavesdropping on the communications. Compl. ¶ 4 ("Consumers reasonably expect that information related to their medical prescriptions will remain confidential."), *id.* ¶ 74 ("Plaintiff's and Class members' communications to ReflexMD, including their sensitive personal and health information, such as prescription information, were confidential communications for purposes of § 632, because Plaintiff and Class Members had an objectively reasonable expectation of privacy in this data."), *id.* ¶ 87 ("This invasion of privacy was serious in nature, scope, and impact, because it related to patients' private medical communications.").

Defendant challenges several of the elements of Plaintiff's CIPA § 632(a) claim, but none of Defendant's arguments have merit. *First*, Defendant argues that it did not intend to record Plaintiff's confidential communications. MTD at 14-15. That is wrong. Defendant intended to record Plaintiff's confidential communications because the very purpose of the LinkedIn Insight Tag is to record consumers' interactions with the Website. Compl. ¶¶ 21-27, 38, 43-45. As mentioned above, the RelexMD Website has one purpose, to sell prescription medications to customers and ensure that they qualify for the medication by collecting private health information regarding that customer. Compl. ¶ 35. The LinkedIn Insight Tag also has a specific purpose, namely, to intercept and record a consumer's interaction with a website. Compl. ¶ 7. Defendant nevertheless permitted ReflexMD to install the LinkedIn Insight Tag and LinkedIn itself used that confidential information by incorporating it into its algorithms for the purpose of creating targeted audience groups and selling advertising on its platform. *Id.* ¶ 38.

Rojas v. HSBC Card Servs. Inc., 20 Cal. App. 5th 427 (2018) is instructive. There, the plaintiff brought suit under CIPA §§ 632 and 632.7 because the defendant "employed a full-time telephone call recording system" which was "activated when an employee placed a telephone call" and recorded personal calls made by the plaintiff without consent. *Id.* at 430. The defendant argued "it did not intend to record any specific call that, in fact, contained Rojas's confidential communications, and [. . .] that it did not intend to record any specific call between Rojas and her

daughter." *Id.* at 433. The court rejected the defendant's argument, finding that "neither position is defensible." *Id.* The court accepted the plaintiff's argument that "because HSBC was using, and knew it was using, a full-time telephone call recording system that recorded *all calls* during the period of time when HSBC recorded the 317 conversations at issue, HSBC *intentionally* recorded the calls that contained Rojas's confidential communications—in violation of both sections 632(a) and 632.7(a)." *Id.* The court concluded the defendant "did not meet its burden of establishing as a matter of law that it did not have 'knowledge to a substantial certainty that [its] use of the equipment w[ould] result in the recordation of a confidential conversation' of an employee and a third party like Rojas." *Id.* at 436 (quoting *People v. Superior Ct. of Los Angeles Cnty.*, 70 Cal. 2d 123, 134 (1969)). So too here, Defendant's LinkedIn Insight Tag was activated when Plaintiff and class members navigated to the Website, and it recorded all communications with the Website indiscriminately, including those involving Plaintiff's and class members' private health information, in violation of Cal. Penal Code § 632(a).

Defendant argues that its alleged "policies specifically prohibiting advertising customers from sending sensitive information via the Insight Tag" undermine Plaintiff's claim. MTD at 15. That is wrong. Defendant made no effort to rectify the fact that ReflexMD was using the LinkedIn Insight Tag to transmit confidential information to Defendant, nor did Defendant destroy any such information; on the contrary, Defendant willingly incorporated the information into its algorithms and used it for the purpose of augmenting its advertising machinery, and used Plaintiff's and class members' private health information as a means of targeting them for advertising. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 827–28 (N.D. Cal. 2020) ("[T]he Court finds that Defendants' failure to rectify the defect causing 'false accepts' or destroy the recordings produced under such circumstances could plausibly be considered 'intentional' rather than 'a result of accident or mistake.'"); *Meta Platforms*, 690 F. Supp. 3d at 1076 ("While plaintiffs acknowledge that Meta may tell third parties and Facebook users that it intends to prevent receipt of sensitive health information, plaintiffs contend that is not what Meta *really* intends. . . What Meta's true intent is, what steps it actually took to prevent receipt of health information, the efficacy of its filtering tools, and the technological feasibility of implementing other measures to prevent the transfer of health

information, all turn on disputed questions of fact that need development on a full evidentiary record. . . At this stage, intent has been adequately alleged.").

Second, Defendant argues that the LinkedIn Insight Tag is not a "device" under CIPA. MTD at 15-16. As Defendant acknowledges, however, numerous courts have held that software code such as the LinkedIn Insight Tag qualifies as a device under CIPA. *Meta Platforms*, 690 F. Supp. 3d at 1080 ("I agree that the Pixel software is a device under section 632(a)").

Indeed, this Court has recently held that software constitutes a "device" under CIPA, finding the *Doe v. Meta Platforms* decision persuasive:

> Recent decisions in this Circuit have rejected Apple's interpretation and found that "software is a device under section 632(a)." *Doe v. Meta Platforms, Inc.*, 2023 WL 5837443, at *7 (N.D. Cal. Sept. 7, 2023); *see also Yockey v. Salesforce, Inc.*, No. 22-CV-09067-JST, 2024 WL 3875785, at *7 (N.D. Cal. Aug. 16, 2024) (agreeing that "software qualifies as a device under Section 632" and collecting cases). The Court finds those decisions persuasive. Plaintiffs have plausibly alleged that the Apple Apps at issue in this case constitute a "device" under Section 632.

Libman v. Apple, Inc., 2024 WL 4314791, at *13 (N.D. Cal. Sept. 26, 2024) (Davila, J.).

Third, Defendant argues "Plaintiff does not plausibly allege that her online communications with ReflexMD were 'confidential' within the meaning of the statute." MTD at 16. Defendant's argument is meritless. Plaintiff navigated to the Website for the sole purpose of purchasing *prescription medication*, and in doing so provided *private health information* in order to qualify for the medication. Compl. ¶ 6. As indicated above, health information is among the most private and confidential information there is, and individuals such as Plaintiff who disclose private health information to a health care provider reasonably expect that the information will be kept private between Plaintiff and the provider.

Defendant next argues that internet-based communications do not give rise to an expectation of privacy. MTD at 16. But courts have recognized an exception where, as here, the information disclosed is protected health information:

> Communications made in the context of a patient–medical provider relationship are readily distinguishable from online communications in general for at least two reasons. First, patient-status and medical-

> related communications between patients and their medical providers are protected by federal law. *See, e.g.*, 42 U.S.C. § 1320d-6 (providing criminal and civil penalties for disclosing protected health information without authorization); 45 C.F.R. § 164.508 (requiring a "valid authorization" for use or disclosure of protected health information); Section I.A.2 *supra* (finding that patient status is protected health information under HIPAA). Second, unlike communications made while inquiring about items of clothing on a retail website, *Revitch*, 2019 WL 5485330, at *3, health-related communications with a medical provider are almost uniquely personal. "One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up." *Norman-Bloodsaw v. Lawrence Berkeley Lab'y*, 135 F.3d 1260, 1269 (9th Cir. 1998) … For these reasons, it seems to me that plaintiffs will likely be able to show that they had an objectively reasonable expectation that their communications with their medical providers were confidential.
>
> Accordingly, plaintiffs will likely be able to show that the communications at issue here were confidential under the CIPA.

In re Meta Pixel Healthcare Litig., 647 F. Supp. 3d 778, 799 (N.D. Cal. 2022) (internal citations omitted).

C. Plaintiff Adequately Alleges That Defendant Intercepted the "Content" of Her Communications with The Website

Relying exclusively on non-binding authority from Massachusetts that considered a Massachusetts statute (and not CIPA), Defendant argues that Plaintiff has not alleged the interception of "content." MTD at 16-17. Defendant's argument is at odds with well-established CIPA case law.

As discussed above, California courts have interpreted CIPA consistent with the federal Wiretap Act, which defines "Contents" as "any information concerning the substance, purport, or meaning of [a] communication.'" *See* 18 U.S.C. § 2510(8); *Brodsky*, 445 F. Supp. 3d at 127. Courts have routinely found that "contents" include information conveyed to a website involving protected health information. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 784 (finding that the defendant intercepted the "contents" of the plaintiff's communications where the plaintiff's "information, which is contemporaneously redirected to Meta, revealed their status as patients and was monetized by Meta for use in targeted advertising"); *id.* at 798 ("Meta mounts a single challenge to a single element here, arguing that plaintiffs cannot show that the intercepted information is "content" based on its arguments under the federal Wiretap Act. . . For the reasons given above, this

challenge fails."); *Cousin v. Sharp Healthcare*, 702 F. Supp. 3d 967, 976 (S.D. Cal. 2023) ("Plaintiffs allege that their data included personal search queries—such as specialty healthcare providers and treatments for medical conditions—and therefore plausibly conveyed content: their PHI.").

Defendant argues that Plaintiff conveyed mere "routine browsing information" (MTD at 16-17), but Defendant's argument is belied by the factual allegations of the Complaint, which make clear that Defendant intercepted Plaintiff's "click" events which "detail information about which page on the ReflexMD Website the patient was viewing as well as the selections they were making" (Compl. ¶ 43), as well as "communications that contained confidential prescription information" (*id.* ¶ 6). Plaintiff's and class members' interactions with the Website "reveal specific information about [the] user's queries [and] reflect the 'contents' of a communication." *St. Aubin*, 2024 WL 4369675, at *4. That is sufficient.

D. Plaintiff States a Claim for Invasion of Privacy Under the California Constitution

To state a claim for invasion of privacy under the California Constitution, Plaintiff "must show that (1) [she] possess[es] a legally protected privacy interest, (2) [she] maintain[s] a reasonable expectation of privacy, and (3) the intrusion is 'so serious ... as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (quoting *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)).

First, Plaintiff has a legally protected privacy interest in her protected health information, which was intercepted by Defendant. *Norman-Bloodsaw v. Lawrence Berkeley Lab'y*, 135 F.3d 1260, 1269 (9th Cir. 1998) ("The constitutionally protected privacy interest in avoiding disclosure of personal matters clearly encompasses medical information and its confidentiality."). As discussed above, Plaintiff's health information is protected by federal law. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 799; 42 U.S.C. § 1320d-6; 45 C.F.R. Part 160 and 164. In a similar case involving an embedded software pixel on the webpage of a health care provider, the court found the plaintiffs had a protected privacy interest in health-related information disclosed to an online health care provider:

> HIPAA defines "protected health information," or "PHI" as "individually identifiable" information that is "created or received by a health care provider" and that "[r]elates to the past, present, or future physical or mental health or condition of an individual" or the "provision of health care to an individual." 45 C.F.R. § 160.103. Having reviewed Plaintiffs' allegations, [. . .]the Court finds that their interactions on Defendant's website, while "unauthenticated" or publicly facing, plausibly involve PHI. As to whether the information is individually identifiable, all three Plaintiffs plead that they are Facebook users. . . Plaintiffs allege at length how Meta Pixel uses JavaScript code to connect internet activity to a specific individual using IP addresses and Facebook credentials. . . Turning to the information that is tracked and whether it is protected, Plaintiff Cousin alleges that she used Sharp's website to search for a primary care physician. . .

Cousin, 702 F. Supp. 3d at 973.

So too here, Plaintiff's communications with the Website contained PHI (including interacting with the survey on the Website and purchasing prescription medication). Further, Defendant embedded the LinkedIn Insight Tag (using JavaScript code) which transmitted Plaintiff's private health information back to it for purposes of augmenting Defendant's marketing algorithms.

Defendant does not question the fact that Plaintiff and class members have a protected privacy interest in their private health information. Instead, Defendant simply rehashes its argument that Plaintiff does not sufficiently allege that her private health information was implicated in Defendant's interception (MTD at 18-20), but that argument fails for the reasons set forth in Section III.A.3., above. Further, Defendant argues that "a close read of Plaintiff's specific allegations reveals that the challenged information is neither particularly sensitive nor private, and is generic, limited to a consumer's interest in" seeing if they qualify for the Semaglutide medication. MTD at 19-20. That is wrong, even on its own terms. The Complaint makes clear that "LinkedIn used this software to track Plaintiff and intercept her communications with ReflexMD, including communications that contained confidential prescription information" such as her purchase of the medication (Compl. ¶ 6). Further, because the LinkedIn Insight Tag captured all of Plaintiff's "click" events on the Website, it necessarily captured her responses to ReflexMD's pre-screening survey which determined whether Plaintiff was eligible to purchase the medication, which constitutes protected

health information. *Id.* ¶¶ 37-43; *see also* 42 U.S.C. § 1320d ("The term 'health information' means any information, whether oral or recorded **in any form or medium**, that-- **(A)** is created **or received** by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and **(B) relates to the past, present, or future physical or mental health or condition of an individual**, the provision of health care to an individual, or the past, present, **or future payment for the provision of health care to an individual**.") (emphasis added); *Robbins v. Mscripts, LLC*, 2023 WL 5723220, at *1 (N.D. Cal. Sept. 5, 2023) (finding that protected health information included "name, date of birth, address, insurance, **and prescription medications**") (emphasis added).

Defendant continues that "Plaintiff's specific allegations establish that LinkedIn does not even receive information showing that a consumer actually purchased Semaglutide, but only that they made some payment on ReflexMD's website." MTD at 20. But "Semaglutide is the only product offered for sale on the Website" (Compl. ¶ 35) and therefore any purchase on the Website necessarily conveys that it was a purchase of Semaglutide.

Second, Plaintiff had a reasonable expectation of privacy that her health-related interactions with an online health care provider would be confidential. The Ninth Circuit recognized in *Facebook Internet Tracking* that "individuals maintain the expectation that entities will not be able to collect . . . broad swaths of personal information absent consent." 956 F.3d 589, 604 n.7 (9th Cir. 2020). "The question is not necessarily whether Plaintiffs maintained a reasonable expectation of privacy in the information in and of itself," but "whether the data itself is sensitive *and* whether the manner it was collected . . . violates social norms." *Id.* at 606 (emphasis in original) (rejecting the suggestion "that Plaintiffs need to identify specific, sensitive information that Facebook collected").

Applying the Ninth Circuit's analysis in *Facebook Internet Tracking*, the court in *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 800, a factually analogous case, found that the plaintiffs there "had an objectively reasonable expectation that their communications with their medical providers were confidential based on the laws and regulations protecting the confidentiality of medical information." This analysis applies with equal weight to Plaintiff's communications with

ReflexMD, a medical provider to whom Plaintiff disclosed information to obtain a prescription medication.

Defendant reiterates its argument attempting to cast Plaintiff's interactions with the Website as mere "online commercial activity" (MTD at 21), but that argument fails for the reasons set forth in Section III.B. *See In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 799 (distinguishing private health information sent over the internet from mere routine commercial behavior and noting that disclosure of private health information over the internet is properly considered confidential).

Next, Defendant argues that the generalized disclosures in its Privacy Policy somehow diminish Plaintiff's reasonable expectation of privacy. MTD at 22. However, even assuming that Plaintiff were placed on reasonable notice of LinkedIn's purported Privacy Policy, it makes no mention of LinkedIn intercepting the private health information of Plaintiff and class members and does not state that Plaintiff will be wiretapped when visiting the website of a healthcare provider such as ReflexMD. Indeed, LinkedIn's Privacy Policy expressly states that it "will only collect and process personal data about you where we have lawful bases" (Compl. ¶ 32), giving Plaintiff and class members the reasonable belief that it will not intercept, receive, and use their protected health information, when in fact it does.

Third, Defendant's conduct was highly offensive. As a threshold matter, "questions of whether conduct is 'egregious,' 'offensive,' or violates 'social norms' tend by their very nature to be subjective . . . [and] these questions are typically more appropriately resolved by a jury." *Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1139 (E.D. Cal. 2021); *see also In re Google Location Hist. Litig.*, 514 F. Supp. 3d 1147, 1157 (N.D. Cal. 2021) ("Whether [defendant's] collection and storage of location data when Location History was set to off was highly offensive to a reasonable person is a question of fact.") (citing *Facebook Internet Tracking*, 956 F.3d at 606). Indeed, the Ninth Circuit held that this determination "requires a holistic consideration of factors" and raises "an issue that cannot be resolved at the pleading stage." *Facebook Internet Tracking*, 956 F.3d at 606.

Here, Plaintiff has identified sufficient facts to survive a motion to dismiss because she pleads that Defendant surreptitiously collected her private health information in unexpected ways (and contrary to Defendant's express assertions in its Privacy Policy). Indeed, under similar

circumstances, the court in *In re Meta Pixel Healthcare Litig.* found:

> There is support for plaintiffs' position that Meta has behaved egregiously. By enacting criminal and civil statutes forbidding the disclosure of protected health information without proper authorization, Congress has made policy decisions regarding the importance of safekeeping this information. *See, e.g.*, 42 U.S.C. § 1320d-6 (providing criminal and civil penalties for disclosing protected health information without authorization); 45 C.F.R. § 164.508 (requiring a "valid authorization" for use or disclosure of protected health information). Courts have also found that taking personal contact information without consent could be deemed highly offensive. *See Opperman v. Path*, 87 F. Supp. 3d 1018, 1060–61 (N.D. Cal. 2014) (finding that a jury must decide whether the "surreptitious theft of personal contact information" is highly offensive). Finally, I note that Meta's policies forbid the transmission of health-related information, which the Ninth Circuit has found to be relevant in the "highly offensive" inquiry. *See In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d at 606 (finding that highly offensive element was sufficiently pleaded where Facebook collected full-string detailed URLs and where "Plaintiffs have alleged that internal Facebook communications reveal that the company's own officials recognized these practices as a problematic privacy issue."). These arguments have merit.

647 F. Supp. 3d at 800–01.

The same analysis applies here. As discussed above, Plaintiff disclosed private health information when interacting with the Website, which is entitled to stringent protections under the law. Further, LinkedIn purports to forbid the transmission of health-related information with regard to the LinkedIn Insight Tag (even though it acts contrary to its stated policy), which reveals that Defendant's own officials recognized that collection of such data is a problematic privacy issue.

Defendant seeks to liken Semaglutide, a prescription medication, with over-the-counter health related products such as "vitamin purchases." MTD at 24. However, records of prescription medications and information concerning the same constitute private health information under federal law, and therefore are entitled to high levels of protection. *Robbins*, 2023 WL 5723220, at *1; 42 U.S.C. § 1320d.

Defendant argues that its conduct was not highly offensive because it allegedly lacked a "culpable motive." MTD at 24. But questions of intent are generally questions of fact. *Oddo v.*

United Techs. Corp., 2022 WL 577663, at *16 (C.D. Cal. Jan. 3, 2022). Further, for the reasons set forth in Section III.B., above, Plaintiff has plausibly plead facts establishing that Defendant acted with intent in eavesdropping on Plaintiff's interactions with the Website, including by permitting ReflexMD, a healthcare provider and retailer of prescription medication, to embed the LinkedIn Insight Tag into its Website, and by using the intercepted information to improve its advertising services and algorithms. *See In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017) (the "collection of intimate or sensitive personally identifiable information may amount to a highly offensive intrusion"). Further, "more routine data collection practices may be highly offensive if a defendant disregards consumers' privacy choices while simultaneously 'h[olding] itself out as respecting' them.'" *Id.* (quoting *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 292 (3d Cir. 2016)). Here, Defendant disguised the LinkedIn Insight Tag as a first-party cookie so it could circumvent third-party cookie blockers and collected Plaintiff's and class members' personal health information despite expressly stating that it "will only collect and process personal data about you where we have lawful bases." Compl. ¶ 32. Therefore, LinkedIn's conduct is egregious because it disregarded consumers' privacy choices while holding itself out as respecting them.

IV. CONCLUSION

For the foregoing reasons, Plaintiff respectfully requests that the Court deny Defendant's Motion to Dismiss.

Dated: November 22, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/ Sarah N. Westcot*
Sarah N. Westcot

Sarah N. Westcot (SBN 264916)
701 Brickell Avenue, Suite 2100
Miami, FL 33133
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: swestcot@bursor.com

Counsel for Plaintiff